IN THE CLAIMS:

1. (Original) A method on an end user system for updating previously stored usage conditions to allow additional copies of previously received encrypted digital content to be made on a computer readable medium, the method comprising the steps of:

receiving a request from a user to create at least one additional copy of previously received encrypted digital content with associated usage conditions;

reviewing the associated usage conditions to determine if at least one additional copy has been authorized; and

creating at least one additional copy onto a computer readable medium of the encrypted digital content, if the at least one additional copy has been authorized.

2. (Original) The method according to claim 1, wherein the step of receiving a request from a user, further comprises the sub-steps of:

sending a request over a telecommunications infrastructure from the end user system to an electronic store for the permission to create at least one additional copy of the previously received encrypted digital content;

receiving from the electronic store a description of the previously received encrypted digital content requested to be copied with an associated hash value; and

comparing the hash value received with a previously stored hash value to determine if they are identical and if the hash value is not identical not authorizing the at least one additional copy to be made.

3. (Original) The method according to claim 1, wherein the step of creating at least one additional copy includes creating at least one additional copy by decrypting the previously received encrypted digital content in a tamper resistant environment so as to deter unauthorized access to the previously received encrypted digital content.

4. (Original) The method according to claim 1, wherein the step of creating at least one additional copy includes creating onto at least one additional copy on a computer readable medium selected from the group of computer readable mediums consisting of recordable CDs, DVDs, ZipDisks™, tape, Flash memory, and RAM.

5. (Original) The method according to claims 1, further comprising the step of receiving encrypted digital content if the additional copy has not been authorized.

6. (Original) The method according to claims 2, further comprising the sub-step of sending payment information from the end user system to the electronic store for payment of the at least one additional copy of the previously received encrypted content.

7. (Original) A method on an end user system for creating additional copies onto at least one computer readable medium of received encrypted content, the method comprising the steps of:

receiving encrypted content with associated usage conditions and a first hash value;

receiving a selection from an end user to create at least one copy of the encrypted content onto at least one computer readable medium;

sending a request to an online electronic store of the encrypted content selected to be copied;

receiving from the electronic store a description of the content selected to be copied along with a second hash value; and

determining if the first hash value received is identical to the second hash value and if the first hash and the second hash value is identical authorizing the creating additional copies onto at least one computer readable medium.

8. (Original) The method according to claim 7, further comprising the step of creating at least one additional copy of the encrypted content onto at least one computer readable medium by decrypting the encrypted digital content in a tamper resistant environment so as to deter unauthorized access to the previously received encrypted digital content.

9. (Currently Amended) A computer program product for content management, the computer program product comprising:

a computer readable medium containing programming instructions for use by an end user information processing system, the programming instructions for updating previously stored usage conditions on ~~an~~ the end user system to allow additional copies of previously received encrypted digital content to be made on a second computer readable medium, the programming instructions for performing the method comprising:

receiving a request from a user to create at least one additional copy of previously received encrypted digital content with associated usage conditions;

reviewing the associated usage conditions to determine if at least one additional copy has been authorized; and

creating at least one additional copy onto a the second computer readable medium of the encrypted digital content, if the at least one additional copy has been authorized.

10. (Original) The computer readable medium according to claim 9, wherein the programming instruction of receiving a request from a user, further comprises the programming instructions of:

sending a request over a telecommunications infrastructure from the end user system to an electronic store for the permission to create at least one additional copy of the previously received encrypted digital content;

receiving from the electronic store a description of the previously received encrypted digital content requested to be copied with an associated hash value; and

comparing the hash value received with a previously stored hash value to determine if they are identical and if the hash value is not identical not authorizing the at least one additional

copy to be made.

11. (Original) The computer readable medium according to claim 9, wherein the programming instruction of creating at least one additional copy includes creating at least one additional copy by decrypting the previously received encrypted digital content in a tamper resistant environment so as to deter unauthorized access to the previously received encrypted digital content.

12. (Original) The computer readable medium according to claim 9, wherein the programming instruction of creating at least one additional copy includes creating onto at least one additional copy on ~~a~~the second computer readable medium selected from the group of computer readable mediums consisting of recordable CDs, DVDs, ZipDisks™, tape, Flash memory, and RAM.

13. (Original) The computer readable medium according to claims 9, further comprising the programming instruction of receiving encrypted digital content if the additional copy has not been authorized.

14. (Original) The computer readable medium according to claims 10, further comprising the programming instruction of sending payment information from the end user system to the electronic store for payment of the at least one additional copy of the previously received encrypted content.

15. (Currently Amended) A computer program product for content management, the computer program product comprising:

a computer readable medium containing programming instructions for use by an end user information processing system, the programming instructions for creating additional copies from onto at least ~~one~~a second computer readable medium of received encrypted content, the programming instructions for performing the method comprising:

receiving encrypted content with associated usage conditions and a first hash value;

receiving a selection from an end user to create at least one copy of the encrypted content onto at least ~~one~~the second computer readable medium;

sending a request to an online electronic store of the encrypted content selected to bc copied;

receiving from the electronic store a description of the content selected to be copied along with a second hash value; and

determining if the first hash value received is identical to the second hash value and if the first hash and the second hash value is identical authorizing the creating additional copies onto at least ~~one~~the second computer readable medium.

16. (Currently Amended) The computer readable medium according to claim 15, further comprising the step of creating at least one additional copy of the encrypted content onto at least ~~one~~the second computer readable medium by decrypting the encrypted digital content in a tamper resistant environment so as to deter unauthorized access to the previously received encrypted digital content.

17. (Cancelled)